AIN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCHES OF:	
7 DEVICES CURRENTLY LOCATED AT THE UNITED STATES SECRET SERVICE EVIDENCE VAULT	Magistrate No. 21-755
7 DEVICES CURRENTLY LOCATED AT THE UNITED STATES SECRET SERVICE EVIDENCE VAULT	Magistrate No. 21-756

APPLICATION AND AFFIDAVIT IN SUPPORT OF SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, Special Agent James McClure, with the United States Secret Service, being first duly sworn, hereby states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search FOURTEEN electronic devices.

2. Your Affiant is a Special Agent with the United States Secret Service ("Secret Service"), and is currently assigned to the Pittsburgh Field Office in Pittsburgh, Pennsylvania. Your Affiant has been a Special Agent since July of 2018. As a Special Agent, Your Affiant is responsible for investigating violations of law of the United States, including violations of Title 18 of the United States Code, and is authorized under Section 3056 of Title 18 to make arrests for such violations. Your Affiant received specialized training at the USSS James J. Rowley Training Center in Beltsville, Maryland relating to criminal investigations of counterfeit currency, identity theft, bank fraud, and more specifically, access device fraud. Prior to joining the United States Secret Service as a Special Agent, Your Affiant was employed as a Uniformed Division Officer with the United States Secret Service from February 2015 to July of 2018.

3. As a federal law enforcement officer, Your Affiant is authorized to investigate violations of laws of the United States, including the crimes outlined herein, and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation. The statements contained in this Affidavit are based primarily on information gathered by me, the Moon Township Police Department and other USSS Special Agents, as well as my training and experience and review of other documents and records.

PURPOSE OF AFFIDAVIT

5. This Affidavit is submitted in support of an application for a search warrant for the following fourteen electronic devices (hereinafter "**TARGET DEVICES**"): **(1) Space Gray Apple iPhone – IMEI 353901109589616 – SIM Card 8901260012789905974**; **(2) Gray Alcatel TCL LX – IMEI 015416004692050 – SIM Card 8901260025182163629; (3) Black iPhone with Case – Severely cracked front screen**; **(4) Silver LG LM-K300MM – IMEI 356322171406075 – SIM Card 8901260053953201592**; **(5) Space Gray Apple iPad A2152 – Serial Number DMPYV369LMPD**; **(6) Space Gray Apple iPhone with Yellow Case – Cracked back glass**; **(7) Gray LG LM-K500MM – IMEI 355041616069287**; **(8) Black Samsung Galaxy A01 – IMEI 3517671111928114 – Serial Number R9PN907N7GJ**; **(9) Gray LG LM-K500MM – IMEI 355041615148090**; **(10) Rose Gold iPhone 6s – Model A1660 – Cracked front screen**; **(11) Rose Gold iPad – Model A2152 – Serial Number F9FD6013LMPN**; **(12) Gray Fuze Card – in the name of "Marc", with Serial Number P20LM15011654**; **(13) Gray Fuze Card – in the name of "CHRISTOPHER", with Serial Number F20JM1400F6FA**; and a **(14) Gray Fuze Card – in the name of "Brian", with unreadable Serial Number**. All **TARGET DEVICES** are

in the possession of the United States Secret Service, Pittsburgh Field Office. Each search item is listed in Attachment A. This Application seeks permission to search each of the fourteen devices for the things described in Attachment B.

PROBABLE CAUSE

6. On March 1, 2021, the U.S. Secret Service, Pittsburgh Field Office received a call from the Moon Township Police Department (MTPD) requesting assistance with three individuals they had in custody for the unauthorized use of credit card information.

7. MTPD received a call from Eggs N'at, 8556 University Boulevard, Moon Township, Allegheny County, PA, 15108, indicating that a customer paid for a food order with what was determined to be a stolen credit card. The owner of the credit card, a victim who resides in Florida, received a notification on her phone as the card was linked to her CashApp mobile application. The victim contacted the Eggs N'at and advised staff that someone was at their restaurant attempting to use her card without her authorization. Eggs N'at then contacted the Moon Township Police Department.

8. Staff at Eggs N'at advised that the male (later identified as Marc LOUISSAINT) attempted to make payment for the order via credit card. The point of sale (POS) terminal indicated the first credit card he presented was "declined." The second card presented by LOUISSAINT was accepted for payment. This payment is what initiated the notification to the card's owner.

9. MTPD responded to Eggs N'at where they encountered LOUISSAINT (driver), Brian VILNEGRE (back passenger) and Christopher RICHARDSON (front passenger) in a Chevrolet Blazer.

10. MTPD also spoke with the Eggs N'At employee who identified LOUISSAINT as the individual who paid for the order with the stolen credit card information. LOUISSAINT,

VILNEGRE, and RICHARDSON were each arrested on local charges of Identity Theft, Access Device Fraud, Conspiracy, Forgery and Possession of Instruments of a Crime.

11. A search incident to arrest of LOUISSAINT, VILNEGRE, and LOUISSAINT discovered they possessed other re-encoded credit/debit/gift cards with information that did not match what was embossed on the front of the cards. There were also numerous cards, some in the names of other persons, found upon the persons of the three arrested individuals.

12. On this same date, Special Agents Wade Watkins and David Halushka, of the United States Secret Service, Pittsburgh Field Office, responded to MTPD and spoke with Detectives Devin Small and Paul Kavanshansky regarding the arrest of the three suspects. Detectives confirmed the above incident and also provided that MTPD secured phones, cards, etc. from their persons upon their arrest.

13. Detective Kavanshansky advised that he swiped the cards recovered from the individuals to determine if the card numbers contained on the magnetic stripe matched the numbers imprinted on the front of the cards. Detective Kavanshansky provided that some of the cards swiped contained information that did not match. He also provided that cards recovered from LOUISSAINT showed that he previously used the cards at a hotel in the Philadelphia, Pennsylvania area as they traveled from Boston, Massachusetts.

14. Detectives further advised that the three individuals, all from the Boston, Massachusetts area, drove from Boston in an Enterprise rental vehicle, and arrived in Moon Township, Pennsylvania on February 28, 2021. Each checked into their own room at the Hampton Inn, 8514 University Boulevard Moon Township, PA, paying all, or part, of their room fees with prepaid Visa cards. When the cards were maxed out, the three individuals paid with cash to pay the outstanding balance.

15. On March 2, 2021, MTPD advised that they applied for and received search warrants issued by the Allegheny County Court of Common Pleas to search the hotel rooms and rental car.

16. Special Agent Halushka and MTPD responded to the Hampton Inn, 8514 University Boulevard, Moon Township, PA 15108. Hampton Inn identified rooms #206, #208, and #304 as the rooms rented by the three individuals.

17. Room #208 was searched first after entry and clearing of the room. This room was rented by Marc LOUISSAINT. There were numerous items of evidence recovered from the room. On the floor was what looked like a shaving kit that contained a sealed, yellow envelope, which contained numerous Target Visa debit gift cards. The kit also had additional Target gift cards that were still within their original packaging. There were also numerous clothing items found that still had the tags on them as if recently purchased.

18. Room #206 was searched after #208. Room #206 was cleared initially upon the entry to room #208 because they were adjoining rooms and the adjoining door was slightly open and unsecure. Room #206 was rented by Brian VILNEGRE. There was a suitcase in the closet that was within the purview of the search warrant. The suitcase was opened and within it were additional gift cards that were similar in nature to those found in LOUISSAINT's room, a cellular phone (**TARGET DEVICE #2)**, and an iPad (**TARGET DEVICE #5)**.

19. Finally, Room #304 was cleared and searched. This room was rented by Christopher RICHARDSON. Within this room was a satchel that contained an iPad tablet (**TARGET DEVICE #11)** and a substantial amount of additional gift cards. In the top drawer of a nightstand were over 100 Target gift cards in denominations of $100 and $200. The majority of these cards were still in their original packaging. There were additional cards located on the dresser and on the other nightstand.

20. Lastly, a search was conducted of the Chevrolet Blazer, which had a Massachusetts tag number (1NDJ45). The search revealed additional clothing items in the rear hatch of the SUV that were either in their original packaging or still had the price tags on them. There were numerous Target gift cards found throughout the vehicle, including the center console, the door pockets, and the rear passenger area in the seat back pockets and on the floor. There were additional cards contained within small pouch-like bags (fanny packs) in the rear seat area. Included in those packs were FUZE cards (**TARGET DEVICES #12, #13,** and **#14)**, which after some research, are capable of holding up to 30 credit/debit/gift card numbers on them. Because FUZE cards can hold up to 30 cards, fraudsters have the potential to use multiple credit/debit cards for a variety of transactions because there is a button on the FUZE card itself, which allows the user to switch between the cards for purchase transactions. In addition, fraudsters tend to use FUZE cards because they appear less suspicious than carrying around multiple credit/debit cards on one's person. A total of three FUZE cards were found, as well as five additional cellular phones (**TARGET DEVICES #4, #7, #8, #9,** and **#10).** Found along with FUZE cards were adapters that appeared to be able to connect to an electronic device via an Apple lightning port, a USB port, or another device with a standard headphone jack input. These devices appeared to be card swipe/reader accessories. These would allow the user to see pertinent card information, such as the card number, cardholder's name, expiration date (if there is one), and validation code. If a card reader is connected to a payment network to include the Internet, the above information can be provided to individuals that are connected to the network. Within the center console was a Deftun Bluetooth credit card reader/writer. This device would allow the reading and re-encoding of data on the magnetic stripe on the reverse side of credit/debit/gift cards. This also allows a fraudster to conduct

transactions and re-encoding anywhere including a vehicle, so that fraudulent activity can be carried out when moving from retailer to retailer and at any time.

21. Your Affiant, based on knowledge, training, and experience, knows that individuals that utilize compromised credit card data need to be able to encode the stolen card numbers onto other cards that contain a magnetic stripe on the reverse side. This is because they do not possess the victim's actual card.

22. Your Affiant is further aware that in order to accomplish this, individuals will use credit card readers/writers to re-encode cards such as gift cards, expired credit cards, or other cards; and that the use of these readers/writers can be done utilizing a mobile phone or tablet.

23. Your Affiant is further aware that individuals who utilize the FUZE cards must have access to an electronic device such as a mobile phone or tablet that contains a mobile software application that allows the individuals to manage the data that is stored on each FUZE card. Such example devices that are capable of this are the **TARGET DEVICES** seized from LOUISSAINT, RICHARDSON, AND VILNEGRE.

24. A NCIC/NLETS database search indicated that LOUISSAINT, RICHARDSON, and VILNEGRE have criminal histories. In Florida 2018, LOUISSAINT was arrested with charges involving larceny and forgery/embossing a credit card. In Massachusetts 2012, RICHARDSON was arrested for receiving stolen property and "Burglarious Instrument, Make." VILNEGRE, in Massachusetts 2012, was arrested for "Burglarious Instrument, Make" and in 2020 was arrested for "Credit Card Fraud over $250."

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cellular telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. These telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for

example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

26. Based on my training, experience, and research, I know that **TARGET DEVICES #1**, **#2, #3, #4, #6, #7, #8, #9,** and **#10** have capabilities that allow them to serve as "a cellular telephone" and that **TARGET DEVICES #5** and **#11** have the capabilities that allow them to serve as "tablets." All of the **TARGET DEVICES** are capable of connecting to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. There is probable cause to believe that things that were once stored on the **TARGET DEVICES** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. *Forensic evidence.* This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used

it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to commit criminal activity, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e) (2) (B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to

computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICES** described in Attachments A1 and A2 for the things described in Attachment B.

Respectfully Submitted,

/s/ James A. McClure
JAMES A. MCCLURE
Special Agent, USSS

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 6th day of April, 2021.

_____
HONORABLE LISA PUPO LENIHAN
UNITED STATES MAGISTRATE JUDGE
Western District of Pennsylvania

ATTACHMENT A-1
Items to be searched

The items to be searched are as follows:

- **TARGET DEVICE #1**: Space Gray Apple iPhone – IMEI 353901109589616 SIM CARD 8901260012789905974
- **TARGET DEVICE #2**: Gray Alcatel TCL LX - IMEI 015416004692050 – Sim Card 8901260025182163629
- **TARGET DEVICE #3**: Black iPhone With Case – Severely Cracked Front Screen
- **TARGET DEVICE #4**: Silver LG LM-K300MM – IMEI356322171406075 – Sim Card 8901260053953201592
- **TARGET DEVICE #5**: Space Gray Apple iPad A2152 – Serial Number DMPYV369LMPD
- **TARGET DEVICE #6**: Space Gray Apple iPhone With Yellow Case – Cracked Back Glass
- **TARGET DEVICE #7**: Gray LG LM-K500MM – IMEI 355041616069287

ATTACHMENT A-2
Items to be searched

- **TARGET DEVICE #8**: Black Samsung Galaxy A01 – IMEI 3517671111928114 – Serial Number R9PN907N7GJ
- **TARGET DEVICE #9**: Gray LG LM-K500MM – IMEI 355041615148090
- **TARGET DEVICE #10**: Rose Gold iPhone 6S – Model A1660 – Cracked Front Screen
- **TARGET DEVICE #11**: Rose Gold iPad – Model A2152 – Serial Number F9FD6013LMPN
- **TARGET DEVICE #12**: Gray Fuze Card With "Brian" – Serial Number is Unreadable
- **TARGET DEVICE #13**: Gray Fuze Card With "Marc" – Serial Number P20LM15011654
- **TARGET DEVICE #14**: Gray Fuze Card With "Christopher" – Serial Number F20JM1400F6FA

ATTACHMENT B

Items seized in Attachment A are currently in possession of the Pittsburgh Field Office.

1. All records relating to violation of Title 18, Section 1029 (Access Device Fraud) prior to April 1, 2021;
2. Any and all records and information relating to the possession, sale, transfer, use or trafficking account numbers associated with any financial institutions.
3. Any and all records and information relating to the production, purchase, sale or trafficking in fraudulently obtained counterfeit identification documents;
4. Any and all records and information relating to communications between and among MARC LOUISSAINT, BRIAN VILNEGRE, CHRISTOPHER RICHARDSON and any other conspirators concerning the access device fraud;
5. Any and all records and information relating to financial records, books, notes, lists of credit card accounts, track data, or photographs concerning the possession, production, use or trafficking of fraudulent access devices;
6. Any and all records and information relating to equipment and materials used in the transaction and/or production of access device fraud;
7. Any and all machines, tools, materials, software, and or supplies used in the manufacturing or processing of fraudulent access devices;
8. Any and all access devices and identification documents used as a means to commit the violation described above;
9. Computers used as a means to commit the violation described above;
10. Proceeds of the violation described above;

11. For any wireless or cellular telephone whose search is authorized by this warrant, records and information described above may be seized in any format, including:

a. incoming and outgoing call and text message logs;

b. contact lists;

c. photo and video galleries;

d. sent and received text messages;

e. online searches and sites viewed via the Internet;

f. online or electronic communications sent and received, including email, chat, and instant messages;

g. sent and received audio files;

h. navigation, mapping, and GPS files;

i. telephone settings, including speed dial numbers and the telephone number for the subject telephone and related identifying information such as the ESN for the telephone;

j. call forwarding information;

k. messages drafted but not sent;

l. voice messages;

12. Additionally, for any wireless or cellular telephone whose search is authorized by this warrant:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs,

photographs, and correspondence;

b. evidence of the attachment to the device of other storage devices or similar containers for electronic evidence;

c. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

d. evidence of the times the device was used;

e. passwords, encryption keys, and other access devices that may be necessary to access the device;

f. documentation and manuals that may be necessary to access the device or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device;

h. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

i. contextual information necessary to understand the evidence described in this attachment;

j. evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, cloud data, and browsing history.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media

that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.